HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,695	08/31/2001	Sridhar Dathathraya	SLA 1055	2135

7590 06/27/2005

David C. Ripma, Patent Counsel
Patent Counsel
Sharp Laboratories of America, Inc.
5750 NW Pacific Rim Boulevard
Camas, WA 98607

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/944,695	**Applicant(s)** DATHATHRAYA, SRIDHAR	
	Examiner LEYNNA T. HA	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _14 April 2005_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-8,10-25 and 27-35_ is/are pending in the application.

4a) Of the above claim(s) _9 and 26_ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-8,10-25 and 27-35_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-8, 10-25, and 27-35 are pending and remains rejected.

Claims 9 and 26 have been cancelled.

2. This is a Final rejection necessitated by new grounds of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-8, 10-25, and 27-35 are rejected under 35 U.S.C. 103(a) as being unpantable over Mazzagatte, et al. (US 6,862,583), and in further view of DeBry (US 6,385,728).

As per claim 1:

Mazzagatte, et al. discloses in a network of connected devices, a communications security method comprising:

encrypting documents **(col.8, lines 14-15)** with a public key; **(col.8, lines 39 and 66-67)** spooling the encrypted documents to a network connected file server; **(col.6, lines 20-21 and col.6, line 62 – col.7, line 5)**

notifying the printer of encrypted documents spooled on the network file server; **(col.9, lines 26-31)**

at the printer, accepting a private key corresponding to the public key used to encrypt the documents; **(col.4, lines 40-42 and col.10, lines 26-28)**

following the acceptance of the private key, transmitting the encrypted documents to a network connected printer; **(col.10, lines 29-30 and col.11, lines 50-53)**

decrypting the documents with the private key; and, **(col.10, lines 31-39)**

printing the decrypted documents. **(col.11, lines 54-57)**

The server of Mazzagatte is a print node (col.7, lines 39-44) which may be a gateway to one or multiple printers (col.10, lines 43-44) or basically a file server (col.4, lines 31-34), where the print node server receives the encrypted data and identification information using public/private key encryption (col.4, lines 40-42) and sends the encrypted data with the private key (col.10, lines 31-33) to the printer for printing (col.6, lines 63-65). The print node and the printer communicates with one another such that the print node indicates the print job information for the printer to determine which recipient is to receive the printouts from the print queue (col.10, lines 13-14). Although, Mazzagatte teaches encryption of data and includes symmetric or asymmetric (public/private key) algorithms, Mazzagatte did not specifically describe the details of the encrypted data by using the public key.

DeBry includes file servers (col.7, lines 4-5) or a document source which is the owner of the document (col.7, lines 50-55) where the document source creates a certificate to verify the user has correct access privileges (col.5, lines 51-65). Further, DeBry teaches if the encrypted document were to be decrypted on its way to the printer the system could be spoofed by replacing the real printer with software, thus, it would be advantageous to provide a unique public encryption key and decrypt and print the document on the fly (col.10, lines 37-44). Hence, DeBry teaches the document is encrypted with a symmetric key where that key is encrypted using the public key (col.11, lines 2-4) and then the encrypted document is placed on the spool. The encrypted document is sent to the printer along with the key to decrypt the public key to thereby decrypt the document for printing (col.11, lines 6-15).

The invention of Mazzagatte and DeBry uses both symmetric and asymmetric (public/private key) algorithms interchangeably where it is obvious that using either one of these algorithms to encrypt data is not a patentable distinction. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry for encrypting the document with a public key prior to transmission to the printer whereby the private key is used for decryption at the printer of would be to prevent unauthorized printing and spoofing.

As per claim 2: See Mazzagatte on col.4, lines 9-10 and col.6, line 62 – col.7, line 5; discusses encrypting the documents with a public key includes encrypting the documents at a network-connected computer having a public key encryption application wherein transmitting the encrypted documents to a network-connected printer includes transmitting the encrypted documents between the computer, file server, and the printer, through a network.

As per claim 3: See Mazzagatte on col.5, line 14 and col.7, line 65-col.8, line 3; discussing supplying the printer driver encryption software to the computer.

As per claim 4: See Mazzagatte on col.4, lines 54-58 and col.7, lines 33-67; discusses supplying an application to optionally encrypt documents in response to the application, creating a graphical user interface (GUI) dialog box to invoke the document encryption option, and in response to invoking the document encryption option, creating a graphical user interface (GUI) dialog box to request and accept public key information.

As per claim 5: See Mazzagatte on col.9, lines 13-20; discusses generating a plurality of public keys with corresponding private keys, distributing the public keys universally to network-connected computers, and selectively distributing the private keys.

As per claim 6: See Mazzagatte on col.8, lines 32-40 and col.9, line 52-55; discussing the printer has a card reader to read code from SMART cards, wherein selectively distributing the private keys includes distributing the private keys as SMART cards, and wherein accepting a private key includes using the code read by the printer card reader.

As per claim 7: See Mazzagatte on col.8, lines 19-41 and col.10, lines 4-18; discusses selectively distributing alpha-numeric codes, creating a table in the printer to cross-reference private keys with alpha-numeric codes and, wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code.

As per claim 8: See Mazzagatte on col.5, lines 53-65 and col.6, line 62-col.7, line 5; discusses spooling the encrypted documents from the file server to a printer memory, and wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

As per claim 9: Cancelled

As per claim 10: See Mazzagatte on col.7, lines 3-56 and col.9, lines 26-34; discussing in response to accepting the private key, generating a list of documents encrypted with the corresponding public key, creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document, and wherein printing the documents includes printing the documents in response to selecting a document.

As per claim 11: See Mazzagatte on col.4, lines 37-40; discusses transmitting a facsimile transmission and wherein decrypting the documents with the private key includes decrypting the encrypted FAX transmission.

As per claim 12:

Mazzagatte discusses the method for secure communications to a network-connected printer, the method comprising:

receiving documents spooled from the file server **(col.6, lines 20-21 and col.6, line 62 – col.7, line 5)** encrypted with a public key; **(Col.8, lines 14-15 and 39)**

accepting a private key corresponding to the public key used to encrypt the documents; **(col.4, lines 40-42 and col.9, lines 13-20)**

decrypting the documents with the private key; and printing the decrypted documents. **(col.10, lines 31-39)**

The server of Mazzagatte is a print node (col.7, lines 39-44) which may be a gateway to one or multiple printers (col.10, lines 43-44) or basically a file server (col.4, lines 31-34), where the print node server receives the encrypted data and identification information using public/private key encryption (col.4, lines 40-42) and sends the encrypted data with the private key (col.10, lines 31-33) to the printer for printing (col.6, lines 63-65). The print node and the printer communicates with one another such that the print node indicates the print job information for the printer to determine which recipient is to receive the printouts from the print queue (col.10, lines 13-14). Although, Mazzagatte teaches encryption of data and includes symmetric or asymmetric (public/private key) algorithms, Mazzagatte did not specifically describe the details of the encrypted data by using the public key.

DeBry includes file servers (col.7, lines 4-5) or a document source which is the owner of the document (col.7, lines 50-55) where the document source creates a certificate to verify the user has correct access privileges (col.5, lines 51-65). Further, DeBry teaches if the encrypted document were to be decrypted on its way to the printer the system could be spoofed by replacing the real printer with software, thus, it would be advantageous to provide a unique public encryption key and decrypt and print the document on the fly (col.10, lines 37-44). Hence, DeBry teaches the document is encrypted with a symmetric key where that key is encrypted using the public key (col.11, lines 2-4) and then the encrypted document is placed on the spool. The encrypted document is sent to the printer along with the key to decrypt the public key to thereby decrypt the document for printing (col.11, lines 6-15).

The invention of Mazzagatte and DeBry uses both symmetric and asymmetric (public/private key) algorithms interchangeably where it is obvious that using either one of these algorithms to encrypt data is not a patentable distinction. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry for encrypting the document with a public key prior to transmission to the printer whereby the private key is used for decryption at the printer of would be to prevent unauthorized printing and spoofing.

As per claim 13: See Mazzagatte on col.5, line 14 and col.7, line 65-col.8, line 3; discusses decrypting the documents with the private key includes operating the printer in response to publicly distributed printer driver encryption software.

As per claim 14: See Mazzagatte on col.8, lines 32-40 and col.9, line 52-55; discusses the printer has a card reader to read code from SMART cards; and, wherein accepting a private key includes using the code read by the printer card reader as the private key.

As per claim 15: See Mazzagatte on col.8, lines 19-41 and col.10, lines 4-18; discusses storing the private keys in the printer; creating a table in the printer to cross-reference private keys with alpha-numeric codes; and, wherein accepting the private keys includes using the private key referenced by the entered alpha-numeric code as the private key.

As per claim 16: See Mazzagatte on col.5, lines 53-65 and col.6, line 62-col.7, line 5; discussing spooling the encrypted documents from the file server into a printer memory; and, wherein decrypting the documents with the private key includes retrieving the encrypted documents from printer memory.

As per claim 17: See Mazzagatte on col.7, lines 3-56 and col.9, lines 26-34; discusses in response to accepting the private key, generating a list of documents encrypted with a corresponding public key; creating a graphical user interface (GUI) dialog box to invoke the selection of an encrypted document ; and, wherein printing the documents includes printing the documents in response to selecting a document.

As per claim 18: See Mazzagatte on col.4, lines 37-40; discusses receiving documents encrypted with a public key includes receiving encrypted documents transmitted as a facsimile (FAX) transmission; and, wherein decrypting the documents with the private key includes decrypting the encrypted FAX transmission.

As per claim 19:

Mazzagatte discloses communications security system in a network of connected devices, the system comprising:

a computer having a network connection, an input to accept a public key, and an encryption application to supply encrypted documents to the network connection in response to accepting a public key; **(col.4, lines 40-42 and col.9, lines 13-20)**

a network connected to the computer to receive and transmit encrypted documents; and, **(col.3, lines 48-555 and col.8, lines 14-15)**

a file server connected to the network to receive encrypted documents from the computer; and **(col.6, lines 20-21 and col.6, line 62 – col.7, line 5)**

a printer having an input connected to the network to accept encrypted documents from the file server **(col.5, lines 47-50)**, the printer having an input to accept a private key corresponding to the public key used to encrypt the documents at the computer, the printer having a decryption application to decrypt the documents with the private key **(col.9, lines 13-20)**, and the

printer having an output to supply a printout of the decrypted documents.
(col.10, lines 31-39)

The server of Mazzagatte is a print node (col.7, lines 39-44) which may be a gateway to one or multiple printers (col.10, lines 43-44) or basically a file server (col.4, lines 31-34), where the print node server receives the encrypted data and identification information using public/private key encryption (col.4, lines 40-42) and sends the encrypted data with the private key (col.10, lines 31-33) to the printer for printing (col.6, lines 63-65). The print node and the printer communicates with one another such that the print node indicates the print job information for the printer to determine which recipient is to receive the printouts from the print queue (col.10, lines 13-14). Although, Mazzagatte teaches encryption of data and includes symmetric or asymmetric (public/private key) algorithms, Mazzagatte did not specifically describe the details of the encrypted data by using the public key.

DeBry includes file servers (col.7, lines 4-5) or a document source which is the owner of the document (col.7, lines 50-55) where the document source creates a certificate to verify the user has correct access privileges (col.5, lines 51-65). Further, DeBry teaches if the encrypted document were to be decrypted on its way to the printer the system could be spoofed by replacing the real printer with software, thus, it would be advantageous to provide a unique public encryption key and decrypt and print the document on the fly (col.10, lines 37-44). Hence, DeBry teaches the document is encrypted with a symmetric key where that key is encrypted using the public key (col.11, lines 2-4) and then the encrypted document is placed on the spool. The encrypted document is sent to the printer along with the key to decrypt the public key to thereby decrypt the document for printing (col.11, lines 6-15).

The invention of Mazzagatte and DeBry uses both symmetric and asymmetric (public/private key) algorithms interchangeably where it is obvious that using either one of these algorithms to encrypt data is not a patentable distinction. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry for encrypting the document with a public key prior to transmission to the printer whereby the private key is used for decryption at the printer of would be to prevent unauthorized printing and spoofing.

As per claim 20: See Mazzagatte on col.5, line 14 and col.7, line 65-col.8, line 3; discussing the computer includes printer driver encryption software to generate the encryption application; and wherein the printer is operated in response to the printer driver encryptions software loaded in the computer.

As per claim 21: See col.4, lines 57-58 and col.7, lines 33-55; discussing the computer has a display with an input connected to the application, wherein encryption application creates a graphical user interface (GUI) dialog box on the display to optionally invoke the encryption of documents, and in response to invoking the document encryption option, creates a GUI dialog box to request and accept public key information.

As per claim 22: See Mazzagatte on col.7, lines 11-27; discussing a system administrator to generate a plurality of public keys with corresponding private keys, the system administrator distributing the public keys universally to network-connected computers, and selectively distributing the private keys.

As per claim 23: See Mazzagatte on col.4, lines 9-10 and col.9, line 56; private keys configured as code in SMART cards; and, wherein the printer private key input is a card reader to read SMART cards, the printer using the code read by the card reader as the private key.

As per claim 24: See Mazzagatte on col.4, lines 39-41 and col.10, lines 4-20; discussing the system administrator generates a table cross-referencing the private keys to alpha-numeric codes, and selectively distributes the alpha-numeric codes; and, wherein the printer private key input is a keyboard interface to accept private keys referenced by the alpha-numeric code entered on the keyboard, and the printer further comprising a memory to store the private keys, and a table to cross-reference private keys to alpha-numeric codes.

As per claim 25: See Mazzagatte on col.6, line 62-col.7, line 5 and col.11, lines 17-20; discussing the printer includes a memory to spool the encrypted documents received from the file server, the printer decrypting the documents with the private key by retrieving the encrypted documents from printer memory.

As per claim 26: Cancelled

As per claim 27: See Mazzagatte on col.7, lines 13-67 and col.9, lines 26-34; discussing the printer has display connected to the decryption application to depict a list of documents encrypted with a corresponding public key, in response to accepting the private key; wherein the printer decryption application creates a GUI dialog box on the display to invoke the selection of encrypted documents, the printer printing the documents in response to selecting a document from the GUI dialog box.

As per claim 28: See Mazzagatte on col.4, lines 37-40; discussing the computer transmits the encrypted documents as a facsimile (FAX) transmission; wherein the network is a telephone system; and, wherein the printer decrypts the encrypted FAX transmission.

As per claim 29:

Mazzagatte discloses a secure communications network-connected printer, the printer comprising:

a network connection to receive documents from the file server **(col.6, lines 20-21 and col.6, line 62 – col.7, line 5)** encrypted with a public key; **(col.8, lines 39 and 66-67)**

an input to accept a private key corresponding to the public key used to encrypt the documents; **(col.4, lines 40-42 and col.9, lines 13-20)**

an decryption application to decrypt the documents with the private key; and, an output to supply a printout of the decrypted documents. **(col.10, lines 31-39)**

The server of Mazzagatte is a print node (col.7, lines 39-44) which may be a gateway to one or multiple printers (col.10, lines 43-44) or basically a file server (col.4, lines 31-34), where the print node server receives the encrypted data and identification information using public/private key encryption (col.4, lines 40-42) and sends the encrypted data with the private key (col.10, lines 31-33) to the printer for printing (col.6, lines 63-65). The print node and the printer communicates with one another such that the print node indicates the print job information for the printer to determine which recipient is to receive the printouts from the print queue (col.10, lines 13-14). Although, Mazzagatte teaches encryption of data and includes symmetric or asymmetric (public/private key) algorithms, Mazzagatte did not specifically describe the details of the encrypted data by using the public key.

DeBry includes file servers (col.7, lines 4-5) or a document source which is the owner of the document (col.7, lines 50-55) where the document source creates a certificate to verify the user has correct access privileges (col.5, lines 51-65). Further, DeBry teaches if the encrypted document were to be decrypted on its way to the printer the system could be spoofed by replacing the real printer with software, thus, it would be advantageous to provide a unique public encryption key and decrypt and print the document on the fly (col.10, lines 37-44). Hence, DeBry teaches the document is encrypted with a symmetric key where that key is encrypted using the public key (col.11, lines 2-4) and then the encrypted document is placed on the spool. The encrypted document is sent to the printer along with the key to decrypt the public key to thereby decrypt the document for printing (col.11, lines 6-15).

The invention of Mazzagatte and DeBry uses both symmetric and asymmetric (public/private key) algorithms interchangeably where it is obvious that using either one of these algorithms to encrypt data is not a patentable distinction. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine Mazzagatte with DeBry for encrypting the document with a public key prior to transmission to the printer whereby the private key is used for decryption at the printer of would be to prevent unauthorized printing and spoofing.

As per claim 30: See Mazzagatte on col.5, line 14 and col.7, line 65-col.8, line 3; discussing the decryption application is responsive to publicly distributed printer driver encryption software.

As per claim 31: See Mazzagatte on col.8, lines 32-40 and col.9, line 56; discussing the private key input is a card reader to read code from SMART cards.

As per claim 32: See col.4, lines 39-41 and col.10, lines 4-18; the private key input is a keyboard interface to accept an alpha-numeric code; and, the printer further comprising: a memory to store the private keys; a memory to store a table cross-referencing private keys with alpha-numeric codes; and, wherein private key input uses the private key referenced by the alpha-numeric code entered at the printer keyboard.

As per claim 33: See Mazzagatte on col.6, lines 20-21 and col.6, line 62-col.7, line 5; a memory to spool the encrypted documents from the file server, and wherein decryption application retrieves the encrypted documents from printer memory for decryption.

As per claim 34: Mazzagatte discusses the printer of claim 29 further comprising:

a display having an input; **(col.9, lines 65-66)**

wherein the decryption application creates a graphical user interface (GUI) dialog box application on the display to invoke the selection of an encrypted document **(col.9, lines 63-66)**, the GUI generating a list of documents encrypted with a corresponding public key, in response to accepting the private key; and **(col.9, lines 26-34 and 10, lines 31-37)**

wherein the documents are decrypted and printed in response to the documents being selected from the GUI. **(col.7, lines 33-45)**

As per claim 35: See Mazzagatte on col.4, lines 37-40 and col.7, lines 33-45; the network connection is a telephone connection and the encrypted documents are facsimile (FAX) transmissions; and wherein the printer decrypts the encrypted FAX transmission.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
Art Unit 2135

LHa